## WHAT IS CLAIMED IS:

1 1. A method con	nprising:
-------------------	-----------

- sending a message from a client to a server, the message to establish a 2 secure connection; 3
- intercepting the data at a security system associated with the server to 4 perform authentication functions; and 5
- establishing a secure connection if proper authentications are performed. 6
- The method of claim 1, wherein the proper authentications comprise 1 2. determining if the server is authentic if the client has requested 2 authentication. 3
- The method of claim 2, wherein the proper authentications additionally 3. 1 comprise determining if the client is authentic if the server has requested 2 authentication. 3
- The method of claim 1, wherein said proper authentications comprise 1 4. validating digital certificates. 2
- The method of claim 1, additionally comprising decrypting the message if 5. 1 the message is encrypted. 2
- The method of claim 1, wherein the authentication functions comprise: 6. 1

64

the server requesting authentication from the client; 2

3		receiving a cheric certificate from the cheric, and
4		determining if the client is authentic, said determining occurring at the
5		security system on behalf of the server.
1	7.	The method of claim 6, wherein the message comprises a digital signature
2		to validate the identity of the client, and said performing the proper
3		authentications comprises validating the digital signature.
1	8.	A method comprising:
2		receiving on a device associated with a server a client hello message from
3		a client, the client hello message indicating a request to establish a
4		secure connection with the server;
5		in response to the client hello message, the device sending a server hello
6		message on behalf of the server to acknowledge the client hello
7		message;
8		if authentication is requested by at least one of the client and the server,
9		then exchanging authentication information;
10		sending a server hello done message from the device to the client, said
11		sending being done on behalf of the server;
12		receiving a finished message from the client; and
13		sending a finished message to the client from the device, said sending
14		being done on behalf of the server.

1	9.	The method of claim 8, wherein said exchanging authentication
2		information comprises:
3		if the client hello message includes a request for authentication from the
4		server, then sending from the device authentication information to
5		the client on behalf of the server; and
6		if the server requests authentication from the client, then receiving
7		authentication information from the client.
1	10.	The method of claim 8, wherein said sending a finished message to the
2		client from the device on behalf of the server comprises:
3		determining if the client is authentic; and
4		if the client has been authenticated, then establishing a secure connection
5		between the client and the server.
1	11.	The method of claim 10, wherein the authentication information comprises
2		a client certificate, and said determining if the client is authentic comprises
3		validating the client certificate.
1	12.	The method of claim 11, wherein validating the client certificate comprises
2		determining that the client certificate is not on a certificate revocation list.
1	13.	The method of claim 11, wherein the authentication information
2		additionally comprises a digital signature, and said determining if the client
3		is authentic additionally comprises verifying the digital signature.

1	14.	The method of claim 8, additionally comprising decrypting the message if
2		the message is encrypted.
1	15.	An apparatus comprising:
2		an application module to:
3		receive incoming data sent from a client and destined for a given
4		server of a plurality of servers in a data center; and
5		route the data to an authentication module to validate the identity of
6		the client;
7		a wired device authentication module associated with the plurality of
8		servers to:
9		receive the incoming data from the application module if the
10		incoming data is sent using wired authentication information;
11		and
12		authenticate the wired device;
13		a wireless device authentication module associated with the plurality of
14		servers to:
15		receive the incoming data from the application module if the
16		incoming data is sent using wireless authentication
17		information; and
18		authenticate the wireless device;

19		a wired device decryption module associated with the plurality of servers
20		to:
21		receive the incoming data from the application module if the
22		incoming data is encrypted using a wired security protocol;
23		and
24		decrypt the data to plain text; and
25		a wireless device decryption module associated with the plurality of
26		servers to:
27		receive the incoming data from the application module if the
28		incoming data is encrypted using a wireless security
29		protocol; and
30		decrypt the data to plain text.
1	16.	The apparatus of claim 15, wherein the wired device authentication
2		module and the wireless device authentication module additionally support
3		authentication functions for authenticating the given server by:
4		requesting server certificates from a certificate authority;
5		storing the server certificates; and
6		sending at least one of the server certificates to a client in response to the
7		client's request for authentication.
1	17	The apparatus of claim 16, wherein the client is a wireless client, and said

2

2		sending comprises sending a long-lived certificate and a short-lived
3		certificate to the wireless client.
1	18.	The apparatus of claim 16, wherein said requesting server certificates
2		from the certificate authority comprises requesting the server certificates
3		at user-defined intervals.
1	19.	A system comprising:
2		one or more servers to exchange data with clients; and
3		a security system associated with the one or more servers to:
4		support authentication functions for authenticating the identity of the
5		one or more servers; and
6		authenticate the identity of clients requesting a secure connection
7		with the one or more servers.
1	20.	The system of claim 19, wherein said authentication functions for
2		authenticating the identity of the one or more servers comprises:
3		requesting server certificates from a certificate authority; and
4		in response to a client requesting authentication from one of the one or
5		more servers, sending a server certificate to the client.
1	21.	The system of claim 19, wherein said authenticating the identity of clients

Docket No.: 42390P12318X Express Mail Label: EL886507275US

requesting a secure connection with the one or more servers comprises:

3		updating a certificate revocation list (CRL);
4		receiving a client certificate from a client requesting a secure connection
5		with a given one of the one or more servers associated with the
6		security system;
7		determining if the client certificate is on the CRL; and
8		if the client certificate is on the CRL, then denying the client access to the
9		given server.
1	22.	An apparatus comprising:
2		a first means to:
3		receive incoming data sent from a client and destined for a given
4		server of a plurality of servers in a data center; and
5		route the data to a means for validating the identity of the client by
6		authenticating a device associated with the client;
7		a second means to:
8		receive the incoming data from the first means if the incoming data
9		is sent using wired authentication information; and
10		authenticate the wired device;
11		a third means to:
12		receive the incoming data from the first means if the incoming data

13		is sent using wireless authentication information; and
14		authenticate the wireless device;
15		a fourth means to:
16		receive the incoming data from the first means if the incoming data
17		is encrypted using a wired security protocol; and
18		decrypt the data to plain text; and
19		a fifth means to:
20		receive the incoming data from the first means if the incoming data
21		is encrypted using a wireless security protocol; and
22		decrypt the data to plain text.
1	23.	The apparatus of claim 22, wherein the second and third means
2		additionally support authentication functions for authenticating the given
3		server by:
4		requesting server certificates from a certificate authority;
5		storing the server certificates; and
6		sending at least one of the server certificates to a client in response to the
7		client's request for authentication.
1	24.	The apparatus of claim 23, wherein the client is a wireless client, and said
2		sending comprises sending a long-lived certificate and a short-lived

6

7

- 3 certificate to the wireless client.
- The machine-readable medium of claim 23, wherein said requesting server certificates from the certificate authority comprises requesting the server certificates at user-defined intervals.
- 2 A machine-readable medium having stored thereon data representing
  2 sequences of instructions, the sequences of instructions which, when
  3 executed by a processor, cause the processor to perform the following:
  4 receive a message from a client to a server, the message to establish a
  5 secure connection;
  - intercept the data at a security system associated with the server to perform authentication functions; and
- 8 establish a secure connection if proper authentications are performed.
- The machine-readable medium of claim 26, wherein the proper authentications comprise determining if the server is authentic if the client has requested authentication.
- The machine-readable medium of claim 26, wherein the message
  comprises a client certificate to validate the identity of the client, and said
  performing the proper authentications comprises validating the client
  certificate.
- 1 29. The machine-readable medium of claim 26, wherein the authentication functions comprise:

Docket No.: 42390P12318X Express Mail Label: EL886507275US 72

Patent Application

3		the security system requesting authentication from the client on behalf of
4		the server;
5		receiving a client certificate from the client; and
6		determining if the client is authentic, said determining occurring at the
7		security system on behalf of the server.
1	30.	An apparatus comprising:
2		at least one processor; and
3		a machine-readable medium having instructions encoded thereon, which
4		when executed by the processor, are capable of directing the
5		processor to:
6		receive a message from a client to a server, the message to
7		establish a secure connection;
8		intercept the data at a security system associated with the server to
9		perform authentication functions; and
10		establish a secure connection if proper authentications are
11		performed.
1	31.	The apparatus of claim 30, wherein the proper authentications comprise
2		determining if the server is authentic if the client has requested
3		authentication.
1	32.	The apparatus of claim 30, wherein the message comprises a client

2 certificate to validate the identity of the client, and said performing the

3 proper authentications comprises validating the client certificate.